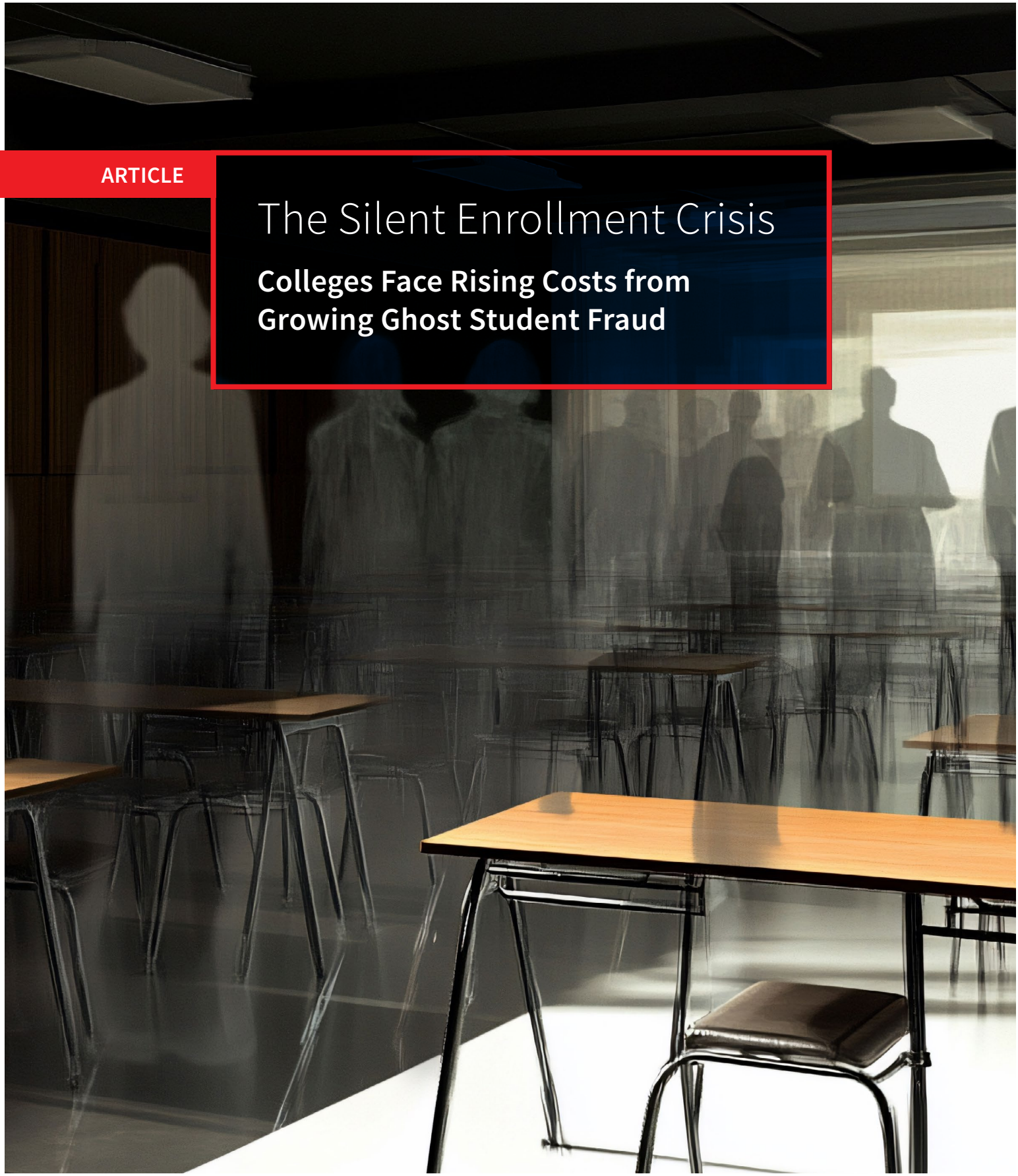
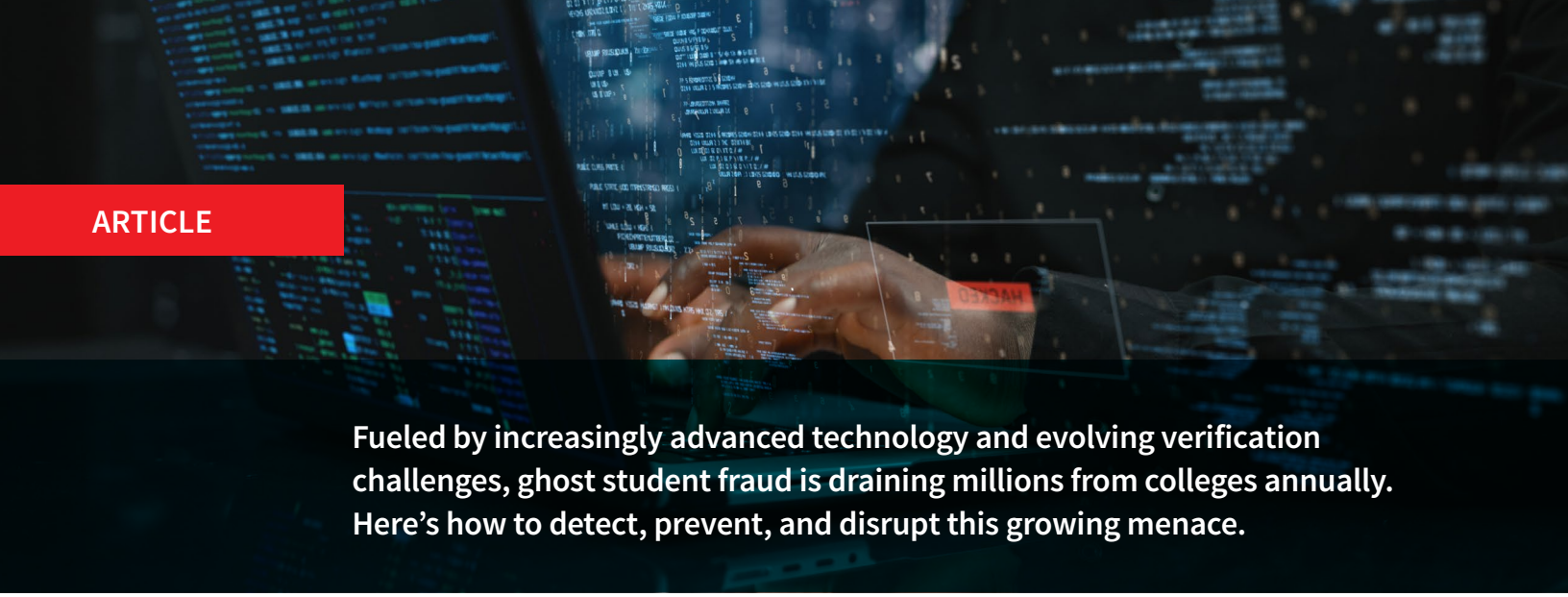
LexisNexis®
RISK SOLUTIONS



ARTICLE

The Silent Enrollment Crisis

Colleges Face Rising Costs from Growing Ghost Student Fraud



ARTICLE

Fueled by increasingly advanced technology and evolving verification challenges, ghost student fraud is draining millions from colleges annually. Here's how to detect, prevent, and disrupt this growing menace.

The Hidden Threat Facing Higher Education

Across the U.S., public community and technical colleges are experiencing a surge in ghost student fraud, and state and private institutions are not exempt from its reach. Leveraging automation, synthetic identities, and digital loopholes, fraudsters infiltrate enrollment systems to access financial aid and institutional resources—often undetected. This growing threat can not only undermine operational integrity, but can also place significant financial strain on higher education institutions.

According to a May 2025 release, the U.S. Department of Education's (DOE) fraud detection systems flagged approximately $90 million in fraudulent or erroneous aid disbursements during the 2024–25 Free Application for Federal Student Aid (FAFSA) cycle.[1] In California alone, community colleges lost $7.6 million in aid to fraudulent identities in the first three quarters of 2024, up from $4.4 million for the entirety of 2023 and $2.1 million the year before.[2]

Inside the Tactics of Ghost Student Schemes

Ghost student fraud is the creation of fake student identities—sometimes using stolen personal data, sometimes completely fabricated—to fraudulently enroll in classes, access campus resources, and most critically, claim financial aid with no intention of attending or completing coursework.

Community colleges are particularly vulnerable due to:

- **Streamlined application processes** with fewer verification steps, and automated or self-service systems.
- **Lower admission barriers**, such as no required essays or interviews, and open admissions.
- **The rise of asynchronous and online learning platforms**—whereby students can access materials (lectures, readings, assignments) on their own schedule, and no real-time interaction is required.

These conditions create a perfect storm for fraudsters looking to exploit volume-based aid systems with little upfront verification.

ARTICLE

How Fraudsters Are Gaming the System

With increasing access to Artificial Intelligence (AI), bad actors are deploying high-tech tools to overwhelm and manipulate academic systems, including:

AI-powered bots that mimic human behavior to navigate admissions processes.

Automated platforms that mass-submit fraudulent applications.

Remote learning environments that limit in-person or biometric verification.

As of early June 2025, the DOE detected **nearly 150,000 suspect identities** on current FAFSA applications, prompting enhanced identity-verification measures for first-time federal aid applicants.[3]

Consequences: Financial, Operational, and Reputational

The damage from ghost student fraud is extensive and deeply disruptive:

Massive financial losses: Approximately $90 million in improper or fraudulent aid distributed during the 2024–25 cycle, not including administrative overhead or system upgrades required to combat fraud.[1]

Operational strain: Fraudulent enrollments skew data, delay real students' access to courses, and overburden staff.

Resource diversion: Financial aid, grants, and institutional support are drained away from legitimate students.

Trust erosion: Repeated incidents of fraud shake public and stakeholder confidence.

ARTICLE

Advanced Countermeasures: A New Era of Fraud Prevention

Evolving beyond traditional defenses can help institutions stay ahead of emerging threats. A multi-layered, technology-enabled strategy is essential, including:

1. Digital Identity Establishment

Leverage solutions that use behavioral analytics and machine learning to validate identity authentication—without adding friction for users.

2. Risk-Based Email Assessment

AI tools can evaluate email domains and behaviors to flag high-risk applications early—before aid is disbursed.

3. Dynamic Authentication

Apply adaptive verification tailored to the risk level of each user interaction. For example, higher-risk sign-ups may prompt additional identity checks, such as multi-factor authentication.

4. Continuous Monitoring

Establish ongoing authentication protocols during student lifecycle events—not just during the admission process.

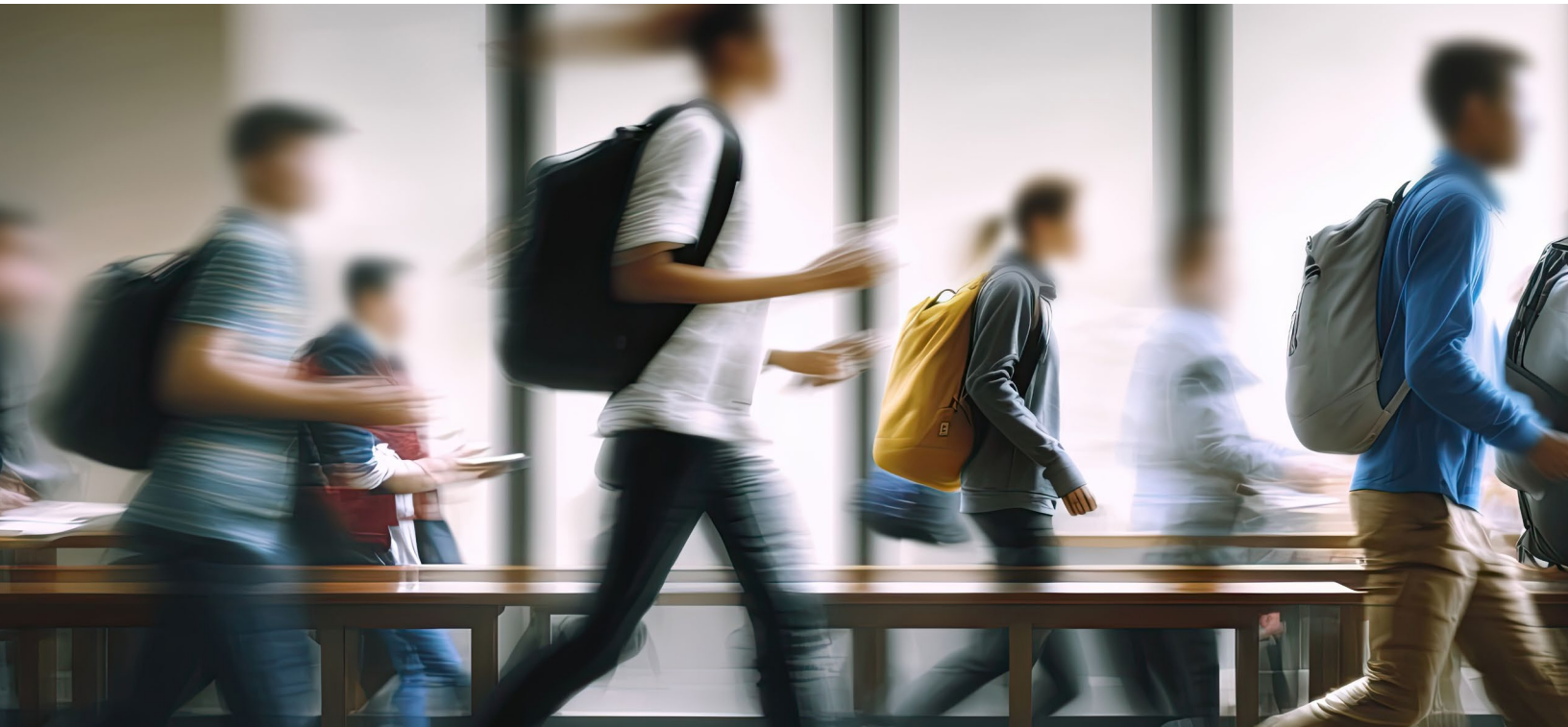
ARTICLE

Staying Ahead of Fraud: Best Practices for Institutions

Colleges and universities can build a more resilient defense with these proactive steps:

- **Deploy AI-powered** fraud detection systems.
- **Share intelligence** across academic institutions and government agencies.
- **Train staff regularly** on evolving fraud tactics and phishing schemes.
- **Conduct periodic audits** of enrollment and financial aid systems.

A collaborative, technology-forward approach is critical to disrupting fraud networks before damage is done.



ARTICLE

Defend the Future of Education

Ghost student fraud doesn't just waste money—it **jeopardizes real students' access** to the education they deserve. As fraud tactics become more advanced, institutions must adapt just as quickly. The path forward lies in embracing advanced identity solutions, AI-powered monitoring, and cross-institutional collaboration.

LexisNexis EssentialID™ is an award-winning, seamless, and secure identity orchestration platform providing colleges multi-layered, fraud-resistant identity verification, third-party data integration, and decision-making capabilities.

Balance Access and Trust

Generate more reliable and actionable outcomes through our **99.99% linking precision rate**.

Protect your college from risk by leveraging our **adherence to strict ethical standards in data use and privacy** and **proven expertise in regulatory compliance**.

Secure your institution today with LexisNexis® Risk Solutions.

LexisNexis® RISK SOLUTIONS

Visit to learn more:
Tel: 1-800-869-0751

1. Investopedia, *Federal Student Aid Fraud Detection Measures Are Reinstated*
2. GovTech, *How AI Is Combating Enrollment Fraud at Community Colleges*
3. Inside Higher Ed, *Stricter ID Verification Required for Federal Aid Applicants*

About LexisNexis® Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com, and www.relx.com.